uCertify

Course Outline

CompTIA CYSA&#43 (CS0-003)

17 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Today's Cybersecurity Analyst

   Chapter 3: System and Network Architecture

   Chapter 4: Malicious Activity

   Chapter 5: Threat Intelligence

   Chapter 6: Reconnaissance and Intelligence Gathering

   Chapter 7: Designing a Vulnerability Management Program

   Chapter 8: Analyzing Vulnerability Scans

   Chapter 9: Responding to Vulnerabilities

   Chapter 10: Building an Incident Response Program

   Chapter 11: Incident Detection and Analysis

   Chapter 12: Containment, Eradication, and Recovery

   Chapter 13: Reporting and Communication

   Chapter 14: Performing Forensic Analysis and Techniques for Incident Response

   Videos and How To
9. Practice Test

   Here's what you get

   Features

10. Live labs
    - Lab Tasks
    - Here's what you get
11. Post-Assessment

1. Course Objective

Master the CompTIA CySA+ (CS0-003) exam with our comprehensive study guide. Whether you're preparing for the exam or seeking to enhance your cybersecurity skills, our course provides valuable insights into the exam objectives. You'll explore a range of cybersecurity domains, from threat intelligence to vulnerability management and forensic analysis. Designed to empower you with real-world knowledge, our course features interactive lessons, quizzes, pre-assessments, post-assessments, and hands-on labs to hone your skills. Unlock your potential and become a certified Cybersecurity Analyst ready to tackle the challenges of the cybersecurity world.

2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

5. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

6. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

7. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

8. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

9. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

10. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been

recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform

2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**
  1. Best Virtual Learning Solution
  2. Best Content Authoring Development or Curation Solution
  3. Best Higher Education Learning Management Solution (LMS)

- **2020**
  1. Best College and Career Readiness Solution
  2. Best Cross-Curricular Solution
  3. Best Virtual Learning Solution

11. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Introduction

- CompTIA
- The Cybersecurity Analyst+ Exam
- What Does This Course Cover?

- Objectives Map for CompTIA CySA+ Exam CS0-003
- Setting Up a Kali and Metasploitable Learning Environment

Chapter 2: Today's Cybersecurity Analyst

- Cybersecurity Objectives
- Privacy vs. Security
- Evaluating Security Risks
- Building a Secure Network
- Secure Endpoint Management
- Penetration Testing
- Reverse Engineering
- Efficiency and Process Improvement
- The Future of Cybersecurity Analytics
- Summary
- Exam Essentials
- Lab Exercises

Chapter 3: System and Network Architecture

- Infrastructure Concepts and Design
- Operating System Concepts
- Logging, Logs, and Log Ingestion
- Network Architecture
- Identity and Access Management
- Encryption and Sensitive Data Protection
- Summary
- Exam Essentials
- Lab Exercises

Chapter 4: Malicious Activity

- Analyzing Network Events
- Investigating Host-Related Issues
- Investigating Service- and Application-Related Issues
- Determining Malicious Activity Using Tools and Techniques
- Summary
- Exam Essentials
- Lab Exercises

Chapter 5: Threat Intelligence

- Threat Data and Intelligence
- Threat Classification
- Applying Threat Intelligence Organizationwide
- Summary
- Exam Essentials
- Lab Exercises

Chapter 6: Reconnaissance and Intelligence Gathering

- Mapping, Enumeration, and Asset Discovery
- Passive Discovery
- Summary
- Exam Essentials
- Lab Exercises

Chapter 7: Designing a Vulnerability Management Program

- Identifying Vulnerability Management Requirements
- Configuring and Executing Vulnerability Scans

- Developing a Remediation Workflow
- Overcoming Risks of Vulnerability Scanning
- Vulnerability Assessment Tools
- Summary
- Exam Essentials
- Lab Exercises

Chapter 8: Analyzing Vulnerability Scans

- Reviewing and Interpreting Scan Reports
- Validating Scan Results
- Common Vulnerabilities
- Summary
- Exam Essentials
- Lab Exercises

Chapter 9: Responding to Vulnerabilities

- Analyzing Risk
- Managing Risk
- Implementing Security Controls

- Threat Classification
- Managing the Computing Environment
- Software Assurance Best Practices
- Designing and Coding for Security
- Software Security Testing
- Policies, Governance, and Service Level Objectives
- Summary
- Exam Essentials
- Lab Exercises

Chapter 10: Building an Incident Response Program

- Security Incidents
- Phases of Incident Response
- Building the Foundation for Incident Response
- Creating an Incident Response Team
- Classifying Incidents
- Attack Frameworks
- Summary

- Exam Essentials
- Lab Exercises

Chapter 11: Incident Detection and Analysis

- Indicators of Compromise
- Investigating IoCs
- Evidence Acquisition and Preservation
- Summary
- Exam Essentials
- Lab Exercises

Chapter 12: Containment, Eradication, and Recovery

- Containing the Damage
- Incident Eradication and Recovery
- Validating Data Integrity
- Wrapping Up the Response
- Summary
- Exam Essentials

- Lab Exercises

Chapter 13: Reporting and Communication

- Vulnerability Management Reporting and Communication
- Incident Response Reporting and Communication
- Summary
- Exam Essentials
- Lab Exercises

Chapter 14: Performing Forensic Analysis and Techniques for Incident Response

- Building a Forensics Capability
- Understanding Forensic Software
- Conducting Endpoint Forensics
- Network Forensics
- Cloud, Virtual, and Container Forensics
- Post-Incident Activity and Evidence Acquisition
- Forensic Investigation: An Example
- Summary
- Exam Essentials

- Lab Exercises

12. Practice Test

Here's what you get

85	2	85
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

13. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

Today's Cybersecurity Analyst

- Creating a Firewall Rule
- Setting Up a Honeypot on Kali Linux

System and Network Architecture

- Installing Docker
- Viewing the Windows File Registry
- Installing the AD FS Role
- Examining PKI Certificates

Malicious Activity

- Confirming the Spoofing Attack in Wireshark
- Performing a DoS Attack with the SYN Flood
- Using Social Engineering Techniques to Plan an Attack
- Using Performance Monitor
- Performing a Memory-Based Attack
- Using Command-line Tools

- Analyzing Malware Using VirusTotal
- Using TCPdump to Capture Packets
- Enabling Logging for Audited Objects
- Examining Audited Events
- Capturing a Packet Using Wireshark

Threat Intelligence

- Examining MITRE ATT&CK

Reconnaissance and Intelligence Gathering

- Using Maltego to Gather Information
- Performing an Intense Scan in Zenmap
- Using Shodan to Find Webcams
- Using Recon-ng to Gather Information
- Identifying Search Options in Metasploit
- Performing Reconnaissance on a Network
- Scanning the Local Network
- Using the hping Program
- Making Syslog Entries Readable
- Performing Zone Transfer Using dig
- Using the netstat Command
- Using the whois Program
- Using nslookup for Passive Reconnaissance

Designing a Vulnerability Management Program

- Using OWASP ZAP
- Consulting a Vulnerability Database
- Conducting Vulnerability Scanning Using Nessus
- Performing Vulnerability Scanning Using OpenVAS
- Performing Session Hijacking Using Burp Suite
- Using Nikto

Analyzing Vulnerability Scans

- Exploiting LFI and RFI Vulnerabilities
- Exploiting a Website Using SQL Injection
- Conducting CSRF Attacks
- Defending Against a Buffer Overflow Attack
- Understanding Local Privilege Escalation
- Performing a MITM Attack
- Detecting Rootkits
- Attacking a Website Using XSS Injection

Incident Detection and Analysis

- Creating a Forensic Image with FTK Imager

Performing Forensic Analysis and Techniques for Incident Response

- Using EnCase Imager
- Observing an MD5-Generated Hash Value
- Analyzing Forensics with Autopsy
- Observing a SHA256-Generated Hash Value
- Cracking Passwords Using Cain and Abel
- Completing the Chain of Custody
- Finding Hard Drives on the System

Here's what you get

53	52	02:06
LIVE LABS	VIDEO TUTORIALS	HOURS

14. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com